Detecting and Recovering the Multi-tap Broken-Path in Ad-hoc Network via Flow-Based Routing

Ashok. P[1] , Satheesh P. S[2], Anandbabu. N[3], Kannan. K[4], Vinoth. M[5]

PG Scholar (Computer Science and Engineering)
Sri Sairam Engineering College, Chennai.

Abstract— Ad hoc network is a temporary network connection that can change locations and configure itself on the fly. Packet may loss in network due to frequent link failure in ad hoc network. In this paper, we maintain log at each router to find out where the loss actually occur and a special scheme used is Flow-Based routing protocol which provides handoff mechanism during link failure. The node then select alternate route to forward the packets without any loss. The significant nodes are assumed and implemented by using LET and RET information of previous node. This model reduces path breaks and ill effects.

Keywords: Log record, RET/LET, flow-based routing, GPS, flow handoff

1. Introduction

The wireless ad hoc network does not have any kind of infrastructure to form network, due to this it had relative congestion in network which leading to packet buffering and continuously degrades the performance in network. In this paper, an *operationally viable* approach used to find out where the loss arises. The key idea is that detecting packet loss is to find where the packet lost in the network. Thus, when a broken link is detected, the multi-hop-handoff mechanisms alleviate the path breaks and by using RET/LET information to provide alternate path to its destination.

2. Protocol

Maintaining logs stating the information about each packet that passes through it. If the actual behavior deviates from the predicted behavior, then a failure has occurred.

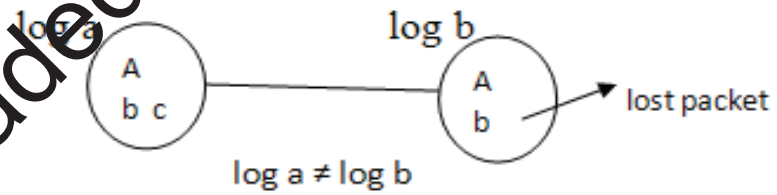

Fig 2.1

Below condition to be satisfied to detect where the packet has lost:

Buffer limit (BL) is maintained at each router. If BL<QP+ps, then the packet P is dropped due to congestion. Every log is evaluated with the previous one before it is forwarded. In our case, if log a ≠ log b, then rb stops forwarding packets further- detect failure.

3. LOG RECORD

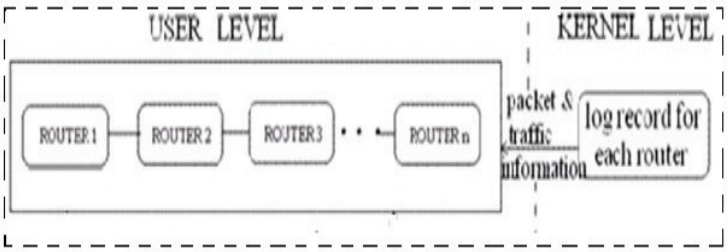

Fig 3.1

Each router in the network maintains a log record containing information about the number of packets sent and received (N), the size of each packet (ps), header of the packet (P), time at which the packet was received (t). This log record helps in detecting where the loss in packet occurred. Each router maintains a queue (Q) before it gets the particular packets. Buffer limit (BL) is maintained at each router. If BL< (qp+ps), then the packet P is dropped. When a packet arrives at router r and is forwarded to a destination that will traverse a path segment ending at router x, r increments an outbound counter associated with router x. Conversely, when a packet arrives at router r, via a path segment beginning with router x, it increments its inbound counter associated with router x. periodically, router x sends a copy of its outbound counters to the associated routers for validation. Then, a given router r can compare the number of packets that x claims to have sent to r with the number of packets it counts as being received from x, and it can detect the number of packet losses.

4. FLOW-ORIENTED ROUTING

Flow-Based Routing Protocol is an on-demand routing protocol that uses a prediction based scheme for selecting and maintaining its routes in case of link failures. FORP uses a unique prediction-based mechanism that utilizes the mobility and location information of each node to estimate the link expiration time (LET). This protocol frequently predict a route expiration time (RET) for given path and select longest likely to live paths and provide handoff mechanism for recently using sessions and find alternate path for transmission of packets before the expiration of currently used path.

5. IMPLEMENTATION

5.1 Route Establishment

5.1.1 Flow-REQ Packet:

When a source node needs to send packet to its destination node, first it checks for availability of route in its own routing table. If it already has an unexpired path, it starts sending packets to its destination. If not, the sender broadcasts a Flow-REQ packet which carries source/destination nodes and flow identification/ sequence number for every session. Upon receiving the packet from its neighbor node, it checks if the sequence number of received Flow-REQ. If sequence number is higher than that of previous node value, it updates address on the packet. If the sequence number is less than that of previously forwarded packet, then the corresponded packet is discarded. Suppose the sequence number same as of pervious identification number, the intermediate node then forwards route request message only if it as arrived through a shorter path.

5.1.2 Flow-Setup Packet:

When Flow-REQ Packet received at the destination node, which contains the list of all nodes it had traversed and along with LET values of each links on that path. FORP assumes all the nodes to be synchronized to a common time by means of GPS information. If the calculated value of RET, corresponding to the new Flow-REQ Packet arrived at the destination, is better than the RET value of the path currently being used, then the destination originates a Flow-SETUP packet. The LET of a link can be estimated given the information about the location, velocity and transmission range of the nodes concerned.

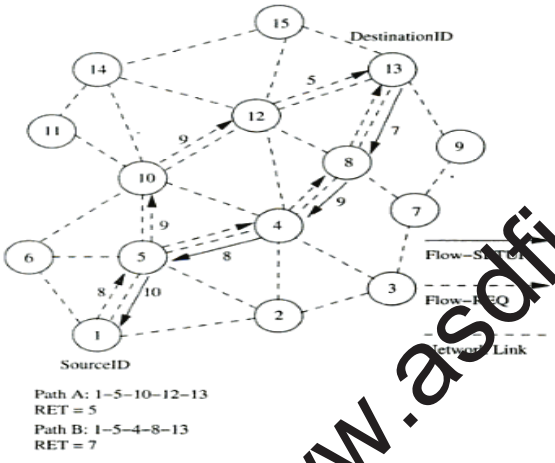

Fig 5.1.1 FORP Route establishment

The route establishment is shown above. In this case, the path 1-5-4-8-13 (path 1) has a RET value of 7, whereas the path 1-5-10-12-13 (path 2) has a RET of 5. This indicates that path 1 may last longer than path 2. Hence the sender node originates a Flow-SETUP through the reverse path 13-8-4-5-1.

5.2 Route Maintenance

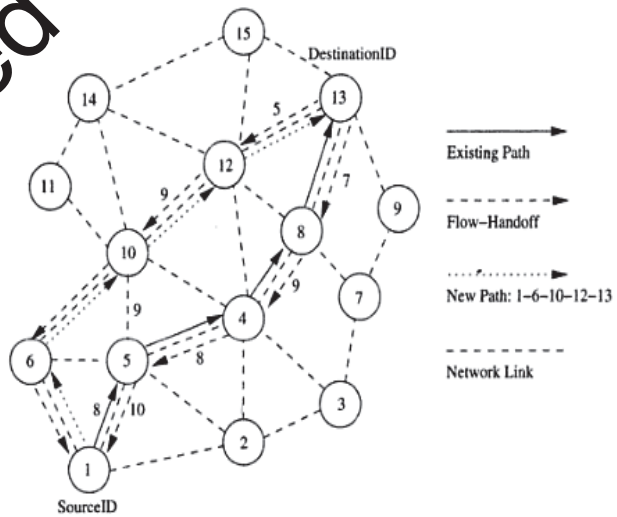

Fig 5.2.1

In the route maintenance, FORP defines a critical time period as the difference between the RET of the currently used path and the time the latest packet take to traverse along the path. This time is also affected by the continuously received RET values form the intermediate nodes along with the data packets. When the destination node determines that a route break is about to occur within a critical time period, it originates a Flow-HANDOFF packet to the source node, which is similar to the Flow-REQ forwarding mechanism. When source node receives many Flow-HANDOFF packet, then it calculates the RET values of each paths, selects the best path and send packets via new path to its destination. In above figure, the Flow-HANDOFF packets are forwarded by every intermediate node after appending the LET information of previous link traversed onto the packet. The existing path 1-5-4-8-13 is erased and new path 1-6-10-12-13 is chosen which is based on the RETs corresponding to different paths traversed by that Flow-HANDOFF packets.

6. PERFORMANCE EVALUATIOIN

It has following steps.

6.1 Throughput

It is the ratio of bits received to the amount of time taken to travel from source to destination.
T=bits received/time taken

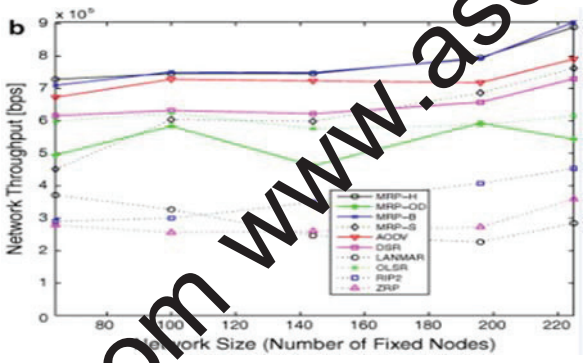

Fig 6.1.1 Comparison of Throughput

6.2 Router Overhead:

It is defined as the average amount of routing protocol control packets in the network.

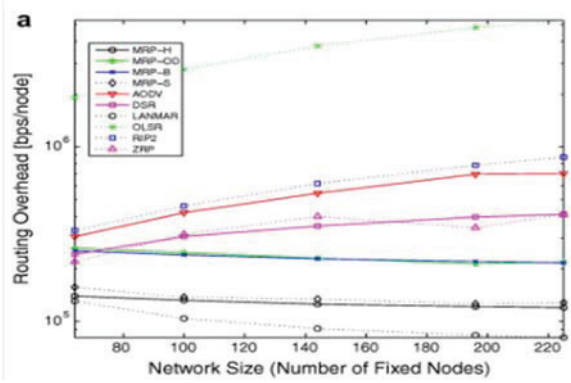

Fig 6.2.1Comparison of Router Overhead

6.3 End-to-end delay:

It is the time taken for a packet to be transmitted across a network from source to destination.

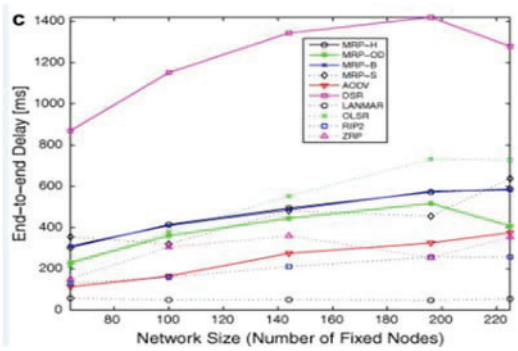

Fig 6.3.1 Comparison of End-to-end delay

7. Conclusion

If any loss of packet in network, log record helps in detecting where the loss in packet occurred and it can be recovered by Flow-Based Routing, which is simulated by using LEF and RET information. The simulation results show that this protocol provide best multi-hop handoff mechanism to recover alternate route in case of link failures.

8. Reference

[1] Ashok, P.; Purushothaman, N.; Elumalai, K., "Detecting and temporarily recovering lost packets in Ad-hoc network by using Bypass routing," Radar, Communication and Computing (ICRCC), 2012 International Conference on , vol., no., pp.264,267, 21-22 Dec. 2012

[2] E. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Personal Communications, vol. 6, no. 2, pp. 46–55, Apr. 1999.

[3] Levente Buttyán, Jean-Pierre Hubaux "Simulating Cooperation in Adhoc Wireless Network" "Mobile Networks and Applications" October 2003.8thvolume

[4] C.E Perkins and E.M Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceeding of IEEE Workshop on Mobile Communication System and Applications 1999, pp. 90-100 Februaru 1999.

[5] V. Padmanabhan and D. Simon. Secure traceroute to detect faulty or malicious routing. In Proc. ACM SIGCOMM HotNets Workshop, Oct. 2002

[6] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", in proc. of 10th International Conference on Network Protocol November 2002

[7] M.K. Marina and S. R. Das, "On demand multipath distance vector routing in ad hoc networks," in IEEE International Conference of Network Protocols (ICNP), 2001.

[8]http://www.scribd.com/doc/37457740/Detecting-Malicious-Packet-Losses

[9]www.ecse.rpi.edu/ "router overhead "

[10] W.Su and M: Gerla, "IPV6 Flow Handoff in Ad Hoc Wireless Networks Using Mobility Prediction," Proceedings of IEEE GLOBECOM 199, pp. 271-275, December 1999.